Range Decompositions and Generalized Square Roots of Positive Semidefinite Matrices

Donald Pierce
Department of Mathematics
Western Oregon State College
Monmouth, Oregon 97361

Submitted by Richard A. Brualdi

ABSTRACT

We establish new connections between the range of a positive semidefinite matrix and its expressions as a finite positive linear combination of Hermitian projections. In particular, if Q is a positive semidefinite matrix and P a Hermitian projection onto any subspace of the range of Q, we provide a method for explicitly calculating the maximal r for which $Q - rP$ is positive semidefinite.

1. INTRODUCTION

In this paper we work with the C^*-algebra $\mathscr{M}_n$ of complex $n \times n$ matrices. By A^* we denote the conjugate transpose of $A \in \mathscr{M}_n$. We call A *positive*, denoted $A \geqslant 0$, if A is positive semidefinite. By e_{ij} we denote the $n \times n$ matrix with a single nonzero entry of 1 in the ijth position, and by span($\{\vec{v}_i\}$) the subspace spanned by the set of vectors $\{\vec{v}_i\}$. By a *projection* we shall mean a Hermitian idempotent.

To understand the structure of $\mathscr{M}_n$ as a C^*-algebra we must understand the structure of the cone of positive matrices. Yet while much is known of the number of projections necessary to write a positive operator A as a positive linear combination of projections (see [1–3]), the spectral theorem remains the only explicit method for doing so. Thus if we desire to write a positive operator as a positive linear combination of projections which are not orthogonal, there is no general way to do so.

655 Avenue of the Americas, New York, NY 10010 0024-3795/91/$3.50

For $A \geqslant 0$ and P a projection onto any subspace of $R(A)$ (the range of A), we give a method for finding all expressions of A as a finite positive linear combination of P and other projections, and characterize those for which the ranges of the projections are orthogonal or linearly independent subspaces. In Section 5 we use these characterizations to give efficient methods for determining the maximal r for which $A - rP \geqslant 0$.

In order to characterize the ways in which $A \geqslant 0$ can be written as a positive linear combination of projections, we exploit two natural correspondences: the first between such expressions of A and the matrices B for which $BB^* = A$, and the second between such matrices and $R(A)$. We begin with some terminology.

By a decomposition of positive $A \in \mathscr{M}_n$ we shall mean any way of writing A as a finite positive linear combination of rank one projections in $\mathscr{M}_n$. That is, $\Sigma_{i=1}^k r_i P_i$ is said to be a *decomposition* of A if $\Sigma_{i=1}^k r_i P_i = A$ with $r_i > 0$ and P_i a projection of rank one in $\mathscr{M}_n$. We consider two decompositions to be equivalent if they are identical up to order of summation.

By an *orthogonal decomposition* we shall mean a decomposition in which the rank one projections are orthogonal, and by a *linearly independent decomposition* one in which no projection is a (complex) linear combination of the others. Observe that if $\vec{v}_i$ is any nonzero vector in $R(P_i)$, $\Sigma r_i P_i$ is a linearly independent decomposition iff $\{\vec{v}_i\}$ is a linearly independent set.

2. RANGE DECOMPOSITIONS

For positive matrices the spectral theorem provides a method for finding orthogonal decompositions: simply break up any spectral projections of rank greater than one. Moreover it is easy to see that the range of each projection in any orthogonal decomposition is an eigenspace, so that every orthogonal decomposition arises in this way.

Certainly nonorthogonal decompositions exist. Indeed, if $A \geqslant 0$ and P is any projection with $R(P) \subseteq R(A)$, it follows from the functional calculus that $A - rP \geqslant 0$ for r the minimum nonzero eigenvalue of A. Thus a positive operator has a decomposition containing the projection onto any one-dimensional subspace of its range.

For P of rank one of the following lemma shows that the maximal r for which $A - rP \geqslant 0$ is obtained precisely when $R(A - rP) \cap R(P) = \vec{0}$ and hence appears as the coefficient of P in any linearly independent decomposition of A containing P.

LEMMA 2.1. *Let $A - rP \geqslant 0$ for P a projection rank one and $r > 0$. Then $A - sP \ngeqslant 0$ for any $s > r$ iff $R(A - rP) \cap R(P) = \vec{0}$.*

Proof. If $R(A - rP) \cap R(P) \neq \vec{0}$, then as P is of rank one, $R(P) \subseteq R(A - rP)$ and $A - sP \geqslant 0$ for $s = r + \lambda$, where λ is the minimum nonzero eigenvalue of $A - rP$. On the other hand, if $R(A - rP) \cap R(P) = \vec{0}$ then $N(A - rP) \nsubseteq N(P)$, and as $((A - sP)\vec{x} \mid \vec{x}) < 0$ for any nonzero $\vec{x} \in N(A - rP) \setminus N(P)$ and $s > r$, it follows that r is maximal. ∎

For a positive operator the existence of a linearly independent decomposition containing the projection onto any one dimensional subspace of its range follows from iterative application of the following theorem of Rosenberg [4, Theorem 2.4].

THEOREM 2.2. *Let $A \geqslant 0$ and S be a subspace of $R(A)$. Then there exists a unique way of writing A as $A = P + Q$ where*:

1. $P, Q \geqslant 0$.
2. $R(P) \cap R(Q) = \vec{0}$.
3. $R(P) = S$, $R(Q) = A(S^{\perp})$.

We wish to point out that for $A \geqslant 0$ it is not in general possible to select more than a single one dimensional subspace of $R(A)$ and obtain a linearly independent decomposition of A containing the projections onto the selected subspaces. Indeed, if $\vec{v}_i$ is a basis vector for $R(P_i)$, then $\Sigma r_i P_i$ is a linearly independent decomposition of A iff $\{\vec{v}_i\}$ is a basis for $R(A)$ satisfying

$$A\left(\operatorname{span}\left(\vec{v}_j\right)^{\perp}\right) \subseteq \operatorname{span}\left(\{\vec{v}_i\}_{i \neq j}\right) \qquad \text{for all } j.$$

3. SQUARE ROOTS OF MATRICES

Recall $A \in \mathscr{M}_n$ is positive iff there exists $B \in \mathscr{M}_n$ such that $BB^* = A$. If B is positive, B is called the *positive square root* of A, is uniquely determined, and is denoted here by $A^{1/2}$.

By an $n \times k$ *square root* of A we shall mean any $n \times k$ matrix B such that $BB^* = A$. For notational convenience we consider only $n \times k$ square roots with $k \geqslant n$, regarding any $n \times k$ square root with $k < n$ as an $n \times n$ matrix by adding $n - k$ additional columns of 0.

For positive $A \in \mathscr{M}_n$ we now define an equivalence relation $\sim$ on the $n \times k$ square roots of A. For $B = (\vec{u}_1 \ \cdots \ \vec{u}_k)$ and $C = (\vec{v}_1 \ \cdots \ \vec{v}_k)$ two $n \times k$ square roots of A, we write $B \sim C$ if after permutation of the columns of C there exist real θ_i such that $\vec{u}_i = e^{i\theta_i}\vec{v}_i$ for each $i = 1, \ldots, k$.

The following theorem establishes the relationship between the square roots of a positive operator and its decompositions.

THEOREM 3.1. *Let $A \in \mathscr{M}_n$ be positive and $\sim$ as defined above. To each decomposition $\Sigma_{i=1}^{k} r_i P_i$ of A and integer $m \geqslant k$, there corresponds a unique equivalence class of $n \times m$ square roots of A. Conversely, to each equivalence class of $n \times m$ square roots of A there corresponds a unique decomposition of A with m or less projections.*

Proof. Suppose we are given a decomposition $\Sigma_{i=1}^{k} r_i P_i$ of A and an integer $m \geqslant k$. For $i = 1, \dots, k$ choose $\vec{v}_i$ to be a unit length basis vector for $R(P_i)$, and set B equal to the $n \times m$ matrix

$$B = \left(\sqrt{r_1}\,\vec{v}_1 \quad \cdots \quad \sqrt{r_k}\,\vec{v}_k \; \vec{0} \quad \cdots \quad \vec{0}\right). \tag{1}$$

Observe

$$BB^* = BI_m B^* = \sum_{i=1}^{m} Be_{ii}B^*$$

$$= \sum_{i=1}^{k} (Be_{ii})(e_{ii}B^*) = \sum_{i=1}^{k} r_i P_i.$$

It is easy to see that interchanging columns of B results only in changing the order of summation in this decomposition.

Conversely, if B is any $n \times m$ matrix such that $BB^* = A$, then $BB^* = \Sigma_{i=1}^{m} Be_{ii}(Be_{ii})^*$ gives a decomposition of A containing m or less projections, since $Be_{ii}(Be_{ii})^*$ is either rank one positive or zero for each i. Note that any B in a given equivalence class gives the same decomposition. ∎

The preceding shows the existence of a decomposition $\Sigma_{i=1}^{k} r_i P_i$ of A is equivalent to the existence of nonzero $\alpha_1, \dots, \alpha_k \in \mathbf{C}$ such that

$$\left(\alpha_1\vec{v}_1 \quad \cdots \quad \alpha_k\vec{v}_k\right)\left(\alpha_1\vec{v}_1 \quad \cdots \quad \alpha_k\vec{v}_k\right)^* = A, \qquad \text{where} \quad \operatorname{span}(\vec{v}_i) = R(P_i).$$

Under this association between square roots and decompositions, the $n \times m$ square root B in (1), where $\vec{v}_i$ is a unit vector in $\mathbf{C}^n$ and $r_i > 0$, corresponds to an orthogonal decomposition of A iff $\{v_i\}_{i=1}^{k}$ is a basis of eigenvectors for $R(A)$ with r_i the eigenvalue associated with $\vec{v}_i$. B corresponds to a linearly independent decomposition iff $\{\vec{v}_i\}_{i=1}^{k}$ is linearly independent.

The following theorem characterizes the square roots of a positive operator and allows us to obtain all square roots of $A \geqslant 0$ from any square root of A. Since a square root of the form in (1) can easily be formed from the spectral decomposition of A, this gives an easy method for finding all the decompositions of a positive operator from its spectral decomposition.

THEOREM 3.2. *Let $A \in \mathcal{M}_n$ be positive and $k \geqslant n$. The $n \times k$ matrix B is an $n \times k$ square root of A iff there exists a $k \times k$ unitary U such that B is the $n \times k$ upper left corner of the $k \times k$ matrix*

$$\begin{pmatrix} A^{1/2} & 0 \\ 0 & 0 \end{pmatrix} U.$$

Proof. Suppose B is an $n \times k$ square root of A. Let B' denote the $k \times k$ matrix obtained from B by adding $k - n$ rows of 0, and $(B'B'^{*})^{1/2}U$ be a polar decomposition of B' with U a $k \times k$ unitary matrix. ∎

An immediate corollary to the above is

COROLLARY 3.3. *Let B be an $n \times k$ square root of $A \geqslant 0$, and C an $n \times m$ square root of A with $m \geqslant k \geqslant n$. Then there exists an $m \times m$ unitary U such that B is the $n \times k$ upper left corner of CU.*

Since our primary interest in the sequel is to find linearly independent decompositions, we shall henceforth restrict ourselves to $n \times n$ square roots, in which case the results of this section may be simplified to:

THEOREM 3.4. *Let $A \in \mathcal{M}_n$ be positive and $\sim$ as defined above. To each decomposition of A, $\Sigma_{i=1}^{k} r_i P_i$, with $k \leqslant n$, there corresponds a unique equivalence class of $n \times n$ square roots of A. Conversely, to each equivalence class of $n \times n$ square roots of A there corresponds a unique decomposition of A.*

THEOREM 3.5. *Let $A \in \mathcal{M}_n$ be positive. The $n \times n$ matrix B is an $n \times n$ square root of A iff there exists a unitary U such that $B = A^{1/2}U$.*

COROLLARY 3.6. *Let B and C be two $n \times n$ square roots of A. Then there exists a unitary U such that $B = CU$.*

4. LINEARLY INDEPENDENT DECOMPOSITIONS

We now give a characterization of those unitary matrices U for which $A^{1/2}U$ corresponds to a linearly independent decomposition.

PROPOSITION 4.1. *Let U be unitary. Then $A^{1/2}U$ corresponds to a linearly independent decomposition of A iff some subset of the columns of U is a basis for $R(A)$.*

Proof. Suppose $U = (\vec{u}_1 \ \cdots \ \vec{u}_n)$ with $\{\vec{u}_i\}_{i=1}^k$ a basis for $R(A)$. As $R(A) = R(A^{1/2})$, $\{\vec{u}_i\}_{i=1}^k$ is also a basis for $R(A^{1/2})$. Since $A^{1/2} \geqslant 0$, $R(A^{1/2})^\perp = \mathcal{N}(A^{1/2})$ (the kernel of $A^{1/2}$), and the nonzero columns of $A^{1/2}U$, $\{A^{1/2}\vec{u}_i\}_{i=1}^k$, form a basis for $R(A^{1/2}) = R(A)$.

On the other hand, if $A^{1/2}U$ corresponds to a linearly independent decomposition of A, then $A^{1/2}U$ has exactly rank(A) nonzero columns—w.l.o.g., $A^{1/2}\vec{u}_1, \dots, A^{1/2}\vec{u}_k$. Since U is unitary, this implies $\{\vec{u}_i\}_{i=k+1}^n$ is an orthonormal basis for $N(A^{1/2})$, whence $\{\vec{u}_i\}_{i=1}^k$ is a basis for $R(A^{1/2}) = R(A)$. ∎

While the preceding provides a method for finding all linearly independent decompositions of a positive $A \in \mathcal{M}_n$, it is possible to avoid computing $A^{1/2}$ by noting that if B is any $n \times n$ square root of A, and U unitary, then BU corresponds to a linearly independent decomposition of A iff BU has exactly rank(A) nonzero columns. Note also that if A is invertible, then every $n \times n$ square root of A corresponds to a linearly independent decomposition.

An interesting corollary is obtained by taking A to be a projection.

COROLLARY 4.2. *Any linearly independent decomposition of a projection is necessarily an orthogonal decomposition.*

Proof. Let $P \in \mathcal{M}_n$ be a projection. If $\Sigma r_i P_i$ is any linearly independent decomposition of P, by Proposition 4.1 it is associated with an $n \times n$ square root of the form PU, where U is a unitary matrix such that some subset of its columns is a basis for $R(P)$. Let $U = (\vec{u}_1 \ \cdots \ \vec{u}_n)$ and assume, w.l.o.g., that $\{\vec{u}_i\}_{i=1}^k$ is a basis for $R(P)$. As P is Hermitian, we have $PU = (\vec{u}_1 \ \cdots \ \vec{u}_k \ \vec{0} \ \cdots \ \vec{0})$, and the decomposition of P associated with PU is orthogonal, since U is unitary. ∎

Since two positive matrices A and B are simultaneously diagonalizable iff they commute, A and B have orthogonal decompositions containing the same projections iff they commute. The following shows that two positive matrices with the same range always have linearly independent decompositions containing the same projections.

PROPOSITION 4.3. *Let A and B be positive with $R(B) \subseteq R(A)$. Then there exists a linearly independent decomposition $\Sigma_{i=1}^k r_i P_i$ of A, and $s_1, \dots, s_m > 0$ with $m \leqslant k$, such that $\Sigma_{i=1}^m s_i P_i$ is a linearly independent decomposition of B.*

Proof. Let A and B be positive with $R(B) \subseteq R(A)$. By changing basis if necessary, we may reduce to the case where A is invertible. In this case $A^{1/2}U$ corresponds to a linearly independent decomposition of A for every unitary U. By Theorems 3.4 and 3.5, the conclusion of this theorem holds iff there exist unitary U, V and a positive diagonal D for which

$$A^{1/2}UD = B^{1/2}V.$$

Or, equivalently, $A^{-1/2}B^{1/2} = UDV^*$. Since every positive operator is of the form UDU^*, the theorem follows from the existence of a polar decomposition of $A^{-1/2}B^{1/2}$. ∎

Generalizing to the case where $R(B) \not\subseteq R(A)$ gives

THEOREM 4.4. *Let A and B be positive with $R(A) \cap R(B)$ a k-dimensional space. Then there exists a linearly independent decomposition $\Sigma r_i P_i$ of A and a linearly independent decomposition $\Sigma s_i Q_i$ of B such that $P_i = Q_i$ for $i = 1, \dots, k$.*

Proof. It follows from Theorem 2.2 that $A = A_1 + A_2$ and $B = B_1 + B_2$, where $A_i, B_i \geqslant 0$, $R(A_1) \cap R(A_2) = R(B_1) \cap R(B_2) = \vec{0}$, and $R(A_1) = R(B_1) = R(A) \cap R(B)$. Applying Proposition 4.3 to A_1, B_1 and finding any linearly independent decompositions of A_2 and B_2 complete the proof. ∎

5. CALCULATING THE MAXIMAL r

We now calculate the maximal r for which $A - rP \geqslant 0$ in case P is of rank one.

PROPOSITION 5.1. *Let $A \geqslant 0$, $\vec{v}$ any unit vector in $R(A)$, and P the projection onto* span$(\vec{v})$. *Then the maximal r for which $A - rP \geqslant 0$ is $r = 1/(\vec{v} \mid \vec{x})$, where $\vec{x}$ is any solution to $A\vec{x} = \vec{v}$.*

Proof. It follows from Lemma 2.1 that the maximal r for which $A - rP \geqslant 0$ will occur as the coefficient of P in any linearly independent decomposition of A containing P. Thus to find r it suffices to find any linearly independent decomposition of A containing P. From Proposition 4.1 any linearly independent decomposition of A corresponds to a square root of the form $A^{1/2}U$, where U is unitary and such that some subset of its columns is a basis for $R(A)$.

Since $\vec{v} \in R(A)$ and any positive operator is invertible on its range, there exists a unique $\vec{x} \in R(A)$ such that $A\vec{x} = \vec{v}$. It follows that any unitary U for which $A^{1/2}U$ has first column $\lambda\vec{v}$ with $\lambda \neq 0$ and which corresponds to a linearly independent decomposition of A has first column $\vec{u} = A^{1/2}\vec{x} / \| A^{1/2}\vec{x} \|$. From the proof of Theorem 3.1 the maximal r for which $A - rP \geqslant 0$ is

$$r = \| A^{1/2}\vec{u} \|^2 = \left\| \frac{A\vec{x}}{\| A^{1/2}\vec{x} \|} \right\|^2 = \frac{1}{\| A^{1/2}\vec{x} \|^2} = \frac{1}{\left(A^{1/2}\vec{x} \mid A^{1/2}\vec{x} \right)} = \frac{1}{\left(A\vec{x} \mid \vec{x} \right)}.$$

■

In order to find the maximal r for which $A - rP \geqslant 0$ in case $\operatorname{rank}(P) > 1$, it is necessary to find linearly independent decompositions of A and P as in Proposition 4.3.

LEMMA 5.2. *Let $A \in \mathcal{M}_n$ be positive of rank m, P a projection of rank k with $R(P) \subseteq R(A)$, and B any $n \times n$ square root of A. Then there exists a unitary U such that BU has exactly m nonzero columns and the first k columns, $\{\vec{v}_i\}_{i=1}^k$, form an orthogonal basis for $R(P)$. Moreover, for any such U the maximal r for which $A - rP \geqslant 0$ is $r = \min\{ \| \vec{v}_i \|^2 : i = 1, \ldots, k\}$.*

Proof. It follows from Proposition 4.3 that A and P have linearly independent decompositions $\Sigma_{i=1}^m r_i P_i$ and $\Sigma_{i=1}^k s_i P_i$, respectively. By Corollary 4.2 the decomposition of P is orthogonal with $s_i = 1$ for all i. If B is any $n \times n$ square root of A, then by Corollary 3.6 there is a unitary U such that BU is associated with the above linearly independent decomposition of A. Note that BU will have exactly m nonzero columns, the first k of which form an orthogonal basis for $R(P)$.

Suppose now that B is any $n \times n$ square root of A, and U any unitary matrix for which BU has exactly m nonzero columns the first k of which, $\{\vec{v}_i\}_{i=1}^k$, form an orthogonal basis for $R(P)$. Then BU is associated with a linearly independent decomposition $\Sigma r_i P_i$ of A, and since $\{\vec{v}_i\}_{i=1}^k$ is an orthogonal basis for $R(P)$, $\Sigma_{i=1}^k P_i$ is an orthogonal decomposition of P.

As $\Sigma r_i P_i$ is a linearly independent decomposition of A, we have $R(A - r_i P_i) \cap R(P_i) = \vec{0}$ for $i = 1, \ldots, k$, and it follows from Lemma 2.1 that the maximal r for which $A - rP_i \geqslant 0$ is r_i. Since $A - rP \geqslant 0$ implies $A - rP_i \geqslant 0$ for $i = 1, \ldots, k$, if $A - rP \geqslant 0$ then $r \leqslant \min\{r_i : i, \ldots, k\}$. With $r = \min\{r_i : i = 1, \ldots, k\}$, clearly $A - rP \geqslant 0$. Hence the maximal r for which $A - rP \geqslant 0$ is $r = \min\{r_i : i = 1, \ldots, k\}$. From the proof of Theorem 3.1 we have $r_i = \| \vec{v}_i \|^2$. Thus the maximal r is $r = \min\{ \| \vec{v}_i \|^2 : i = 1, \ldots, k\}$. ■

THEOREM 5.3. *Let $A \geqslant 0$, P a projection with $R(P) \subseteq R(A)$, $\{\vec{b}_i\}_{i=1}^k$ any orthonormal basis for $R(P)$, and $\vec{x}_i$ any solution to $A\vec{x}_i = \vec{b}_i$. Then the maximal r for which $A - rP \geqslant 0$ is $r = 1/\lambda$, where λ is the largest eigenvalue of*

$$\left(\vec{x}_1 \ \cdots \ \vec{x}_k \ \vec{0} \ \cdots \ \vec{0}\right)^*\left(\vec{b}_1 \ \cdots \ \vec{b}_k \ \vec{0} \ \cdots \ \vec{0}\right).$$

Proof. Let $U = (\vec{u}_1 \ \cdots \ \vec{u}_n)$ be a unitary matrix for which $A^{1/2}U$ has exactly rank(A) nonzero columns with $\{A^{1/2}\vec{u}_i\}_{i=1}^k$ an orthogonal basis for $R(P)$. Since both $\{\vec{b}_i\}_{i=1}^k$ and $\{A^{1/2}\vec{u}_i/\|A^{1/2}\vec{u}_i\|\}_{i=1}^k$ are orthonormal bases for $R(P)$, both

$$\left(\vec{b}_1 \ \cdots \ \vec{b}_k \ \vec{0} \ \cdots \ \vec{0}\right) \quad \text{and}$$

$$\left(\frac{A^{1/2}\vec{u}_1}{\|A^{1/2}\vec{u}_1\|} \ \cdots \ \frac{A^{1/2}\vec{u}_k}{\|A^{1/2}\vec{u}_k\|} \ \vec{0} \ \cdots \ \vec{0}\right)$$

are square roots of P. It follows from Corollary 3.6 that there exists a unitary V such that

$$\left(\vec{b}_1 \ \cdots \ \vec{b}_k \ \vec{0} \ \cdots \ \vec{0}\right)V = \left(\frac{A^{1/2}\vec{u}_1}{\|A^{1/2}\vec{u}_1\|} \ \cdots \ \frac{A^{1/2}\vec{u}_k}{\|A^{1/2}\vec{u}_k\|} \ \vec{0} \ \cdots \ \vec{0}\right).$$

Thus

$$A^{1/2}\left[A^{1/2}\left(\vec{x}_1 \ \cdots \ \vec{x}_k \ \vec{0} \ \cdots \ \vec{0}\right)V\right] = A^{1/2}\left(\frac{\vec{u}_1}{\|A^{1/2}\vec{u}_1\|} \ \cdots \ \frac{\vec{u}_k}{\|A^{1/2}\vec{u}_k\|} \ \vec{0} \cdots \vec{0}\right).$$

Since $A^{1/2}U$ has exactly rank(A) nonzero columns, it is associated with a linearly independent decomposition of A, and hence by Proposition 4.1 $\vec{u}_i \in R(A)$ for $i = 1, \ldots, k$. As the columns of $A^{1/2}(\vec{x}_1 \ \cdots \ \vec{x}_k \ \vec{0} \ \cdots \ \vec{0})V$ are clearly in $R(A)$, it follows that

$$A^{1/2}\left(\vec{x}_1 \ \cdots \ \vec{x}_k \ \vec{0} \ \cdots \ \vec{0}\right)V = \left(\frac{\vec{u}_1}{\|A^{1/2}\vec{u}_1\|} \ \cdots \ \frac{\vec{u}_k}{\|A^{1/2}\vec{u}_k\|} \ \vec{0} \ \cdots \ \vec{0}\right).$$

Since $\| B\|^2 = \| B^*B\|$ for any $n \times n$ matrix B and $\{\vec{u}_i\}_{i=1}^k$ is orthonormal,

$$\left\| \begin{pmatrix} \dfrac{\vec{u}_1}{\| A^{1/2}\vec{u}_1\|} & \cdots & \dfrac{\vec{u}_k}{\| A^{1/2}\vec{u}_k\|}\vec{0} & \cdots & \vec{0} \end{pmatrix} \right\|$$

$$= \left\| \operatorname{diag}\left(\frac{1}{\| A^{1/2}\vec{u}_1\|^2}, \dots, \frac{1}{\| A^{1/2}\vec{u}_k\|^2}, 0, \dots, 0 \right) \right\|$$

$$= \frac{1}{\min\left\{ \| A^{1/2}\vec{u}_i\|^2 : i = 1, \dots, k \right\}}.$$

According to Lemma 5.2 the maximal r for which $A - rP \geqslant 0$ is $r = \min\{ \| A^{1/2}\vec{u}_i\|^2 : i = 1, \dots, k\}$. Thus

$$r = \frac{1}{\left\| A^{1/2}\begin{pmatrix} \vec{x}_1 & \cdots & \vec{x}_k\, \vec{0} & \cdots & \vec{0} \end{pmatrix} V \right\|^2}$$

$$= \frac{1}{\left\| A^{1/2}\begin{pmatrix} \vec{x}_1 & \cdots & \vec{x}_k\, \vec{0} & \cdots & \vec{0} \end{pmatrix} \right\|^2}$$

$$= \frac{1}{\left\| \begin{pmatrix} \vec{x}_1 & \cdots & \vec{x}_k\, \vec{0} & \cdots & \vec{0} \end{pmatrix}^* A \begin{pmatrix} \vec{x}_1 & \cdots & \vec{x}_k\, \vec{0} & \cdots & \vec{0} \end{pmatrix} \right\|}.$$

Since $(\vec{x}_1 \ \cdots \ \vec{x}_k\, \vec{0} \ \cdots \ \vec{0})^* A (\vec{x}_1 \ \cdots \ \vec{x}_k\, \vec{0} \ \cdots \ \vec{0})$ is positive, it follows that $r = 1/\lambda$, where λ is the largest eigenvalue of

$$\begin{pmatrix} \vec{x}_1 & \cdots & \vec{x}_k\, \vec{0} & \cdots & \vec{0} \end{pmatrix}^* A \begin{pmatrix} \vec{x}_1 & \cdots & \vec{x}_k\, \vec{0} & \cdots & \vec{0} \end{pmatrix}$$
$$= \begin{pmatrix} \vec{x}_1 & \cdots & \vec{x}_k\, \vec{0} & \cdots & \vec{0} \end{pmatrix}^* \begin{pmatrix} \vec{b}_1 & \cdots & \vec{b}_k\, \vec{0} & \cdots & \vec{0} \end{pmatrix}. \quad \blacksquare$$

For clarity we now illustrate our procedures for the calculation of a maximal r with an example.

6. EXAMPLE

Consider

$$A = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 3 & 1 \\ 1 & 0 & 1 & 1 \end{pmatrix}.$$

To illustrate Proposition 5.1, let P be the projection onto the subspace spanned by

$$\vec{v} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}.$$

To find the maximal r for which $A - rP$ is positive, we set $A\vec{x} = \vec{v}/\|\vec{v}\|$ and solve for $\vec{x} \in R(A)$. We have

$$(A\vec{x} \mid \vec{x}) = \left(\begin{pmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ 0 \\ \frac{1}{\sqrt{2}} \end{pmatrix} \middle| \begin{pmatrix} \frac{3}{4\sqrt{2}} \\ 0 \\ \frac{-2}{4\sqrt{2}} \\ \frac{3}{4\sqrt{2}} \end{pmatrix} \right) = \frac{3}{4}.$$

Thus the maximal r for which $A - rP \geqslant 0$ is $r = \frac{4}{3}$.

To illustrate Theorem 5.3 let

$$P = \begin{pmatrix} \frac{1}{2} & 0 & 0 & \frac{1}{2} \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ \frac{1}{2} & 0 & 0 & \frac{1}{2} \end{pmatrix}.$$

One obvious orthonormal basis for $R(P)$ is

$$\left\{ \begin{pmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ 0 \\ \frac{1}{\sqrt{2}} \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \right\} = \{\vec{b}_1, \vec{b}_2\}.$$

Setting $A\vec{x}_1 = \vec{b}_1$ and $A\vec{x}_2 = \vec{b}_2$ and solving for $\vec{x}_i \in R(A)$ gives

$$\vec{x}_1 = \begin{pmatrix} \dfrac{3}{4\sqrt{2}} \\ 0 \\ \dfrac{-2}{4\sqrt{2}} \\ \dfrac{3}{4\sqrt{2}} \end{pmatrix} \quad \text{and} \quad \vec{x}_2 = \begin{pmatrix} -\frac{1}{4} \\ 0 \\ \frac{1}{2} \\ -\frac{1}{4} \end{pmatrix}.$$

Then

$$\left(\vec{x}_1\ \vec{x}_2\ \vec{0}\ \vec{0}\right)^*\left(\vec{b}_1\ \vec{b}_2\ \vec{0}\ \vec{0}\right) = \begin{pmatrix} \dfrac{3}{4} & \dfrac{-1}{2\sqrt{2}} & 0 & 0 \\ \dfrac{-1}{2\sqrt{2}} & \dfrac{1}{2} & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix},$$

which has eigenvalues of 1 and $\frac{1}{4}$. Hence the maximal r for which $A - rP \geqslant 0$ is 1.

Part of this material appeared in the author's Ph.D. thesis at University of Colorado Boulder.

REFERENCES

1 Man-Duen Choi and Pei Yuan Wu, Convex combinations of projections, *Linear Algebra Appl.*, to appear.
2 P. A. Fillmore, On sums of projections. *J. Funct. Anal.* 4:146–152 (1969).
3 Y. Nakamura, Any Hermitian matrix is a linear combination of four projections, *Linear Algebra Appl.* 61:133–139 (1984).
4 M. Rosenberg, Range decomposition and generalized inverse of nonnegative Hermitian matrices, *SIAM Rev.* 11:568–571 (1969).

Received 24 July 1989; final manuscript accepted 16 May 1990